السنة: الثامنة المجلد: 08 العدد: 02 ص ص: 243- 266
EISSN 2676-1645 ISSN 2543-375X

علم النفس السيبرياني أداة تشخيص للجريمة الالكترونية قرصنة بيانات المستشفيات أنموذجا للدراسة

Cyber psychology is a diagnostic tool for cybercrime. Data hospital hacking is an example of a study.

حشلافي حميد *، جامعة وهران1
hachelafimed@gmail.com

تاريخ الاستلام:2023/02/17 تاريخ القبول:2023/05/05

ملخص:

تعددت طرق الجرائم الالكترونية وأضحت تشكل خطرا عالميا طالما انها مسحت الحدود، وشملت كل البنية التحتية للمجتمعات سواء في العلاقات الاجتماعية، الاقتصادية والعسكرية. إن التطور التكنولوجي وما انبثق عنه من سرعة تطبيقاته في شتى ميادين الحياة هو ميزة العصر الحديث، ففي الجانب الصحي أضحت استعمالاته تساهم في توفير الأريحية للأطقم والكوادر الصحية في مختلف عمليات التنظيم والتسيير وأيضا في أساليب التشخيص المرضي والطرق العلاجية. بالموازاة، أضحت جحافل الاجرام تصطاد في بركة المعاناة والألم للمرضى بقرصنة بياناتهم الشخصية والتهديد بالتشهير العلني على منصات الفضاء الأزرق.

من أهداف الدراسة: تشخيص نمط الجريمة الإلكترونية التي تخص المؤسسات الاستشفائية وتحديد نمط شخصية المجرم السيبراني.

تتجلى الدراسة في تسليط الضوء على مجموعة من الجرائم السيبريانية التي ركزت على بنوك المعلومات المرتبطة بالحالة الصحية للمرضى، مع تحديد الفترة الزمنية من عمر جائحة كوفيد 19. تم استعمال استمارة تحقيق مبنية على

* المؤلف المراسل

معطيات خصت ظروف الجريمة، مبرراتها ، نمط شخصية المجرم وتحديد طريقة الجريمة.

الكلمات المفتاحية: علم النفس السيبرياني، المجرم السيبرياني، الجريمة الالكترونية، قرصنة البيانات الصحية، القرصنة المعلوماتية.

Abstract:
The methods of cybercrime have multiplied and have become a global threat as long as they initially cleared the borders, and included all the infrastructure of societies, whether in social, economic, and military relations. Technological development and the speed of its applications in various fields of life are the advantage of the modern era. In the health aspect, its uses have contributed to providing comfort to health crews and cadres in various processes of organization and management, as well as in methods of pathological diagnosis and treatment methods, until the patient became diagnosed from a distance. Without the effort of moving from his home or saving tons of his paper files by digitizing his medical file. The study sheds light on the total number of cybercrimes that focused on data banks related to the health status of patients as a sample for the field study. The time for the study was also determined from the age of the COVID-19 pandemic because of the global outbreak of the phenomenon. We used an investigation form based on data that described the circumstances of the crime, its justifications, the criminal's personality type and determining the method of the crime.

Keywords: Cyberpsychology, cybercriminal, electronic crime, piracy of health data, information piracy.

.

مقدمة:

أن التطور الهائل لوسائل التكنولوجيا الرقمية وانعكاساتها في تطوير شبكات التواصل والاتصالات في شتى مجالات الحياة اليومية ساهم في نفس الوقت تغيير في سلوك المستهلك المتكيف مع المعارف لهذه الأنماط الحيوية الحديثة والمتجددة، لكن بالموازاة سمحت بتأهيل وتحديث أساليب الانحراف واستحداث أنواع من الجرائم التي تمردت على قيم المجتمع. بالإضافة الى تعدد الجرائم السيبريانية حتى استحال حصرها من الجانب الاحصائي، طالما"أن الطبيعة العالمية والموزعة على خريطة شبكية للجريمة على الإنترنت تجعل من المستحيل مركزية العد الوطني بواسطة جهاز تقني قادر على إلتقاط جميع الجرائم الإلكترونية، وبالتالي نفهم بشكل أفضل كيف أن صعوبة حصر الظاهرة ووصفها يضعف من مصداقية مؤسسات الدولة" (Benbouzid, 2016).

بالإضافة أن جائحة كوفيد -19 العالمية وانعكاساتها المتعددة الأوجه على نمط حياة الانسان أجبرت الاستعانة بالتكنولوجيا للتغلب على الحواجز الصحية والإدارية التي فرضت جبرا تفاديا للعدوى والإصابات المميتة، فعدلت أوقات العامل من خلال العمل عن بعد(telecommuting) ، والدراسة في مختلف اطوارها عن بعد وحتى التسوق عن بعد(E-commerce) .

أما في مجال الصحة، فقد اعتمدت نفس الابتكارات التكنولوجية والرقمية التي تساهم في الاستشارات الطبية عن بعد " E-health ". وتحقيق المساواة في تلقي الخدمات الصحية والحق في العلاج. إن مبررات تزايد الطلبات على التكنولوجيا الرقمية في القطاع الصحي مثل رقمنة الملف الطبي وحفظ البيانات الشخصية الخاصة بالمرضى من جهة سمحت بآثار إجتماعية واقتصادية جدُ إيجابية للمريض وللمؤسسة الاستشفائية، لكن بالرغم من التحسن المستمر في تأمين بنوك المعلومات والحرص الشديد على حفظها من الاختراق، فقد أصبحت المؤسسات الصحية من بين الأهداف الأساسية للعمل الاجرامي السيبرياني، وقد تفاقم الوضع حتى وصل مستواه الى حدود 600 % خلال جائحة كوفيد-19 (2020,Lederer) . كما أوضح تقرير المكتب الفيدرالي الأمريكي

للتحقيقات من خلال مركز الشكاوى لجرائم الانترنت " IC3"في سنة 2020 والذي قام بتقييد 791.790 شكوى في الولايات المتحدة الامريكية والتي خلفت خسائر بقيمة مالية تقدر ب 4,4 مليار دولار امريكي، في حين قيدت 467.361 شكوى عام 2019 (Federal Bureau of Investigation، 2019).

كما تدعم المؤشرات فيما يخص الاحصائيات العالمية حول عمليات الجرائم السبريانية التي مست المؤسسات الصحية حيث تضاعفت ووصلت الى 730 حادث قرصنة في سنة 2021(2022,Pontier) . كما أشار تقرير لخبراء شركة ويزكاز " WizeCase" سنة 2019 الى عمليات نشر لملفات طبية على البوابة المظلمة مما يقرب 60 جيجابايت من البيانات أو ما يعادل 000 400 26 ملف طبي، بالإضافة لآثار مالية عالمية فاقت 6000 مليار دولار أمريكي فيما يخص الجريمة السيبريانية (Wisecase، 2019).

إن الاستثمارات المالية الهائلة التي اعتمدتها كبرى الشركات العالمية في الصحة الرقمية خلال السنوات الأخيرة، حيث تدل المؤشرات المالية بضخ على سبيل الاستدلال حوالي 350 مليار دولار امريكي سنة 2019 مع تقدير نمو يصل إلى 8 ٪ (2020,Cohen) و مثل هذه الاستثمارات ما اعتمدته شركة جوجل "Google " بالتعاون مع الفدرالية الامريكية للاستشفائيين الجامعيين لعيادة مايو "Mayo Clinic " من اجل الاستعانة في المتابعة الطبية للمرضى بالذكاء الاصطناعي ، كما فتحت شركة أمازون الامريكية " Amazon "عيادة طبية افتراضية لمتابعة صحية لمجموع عمالها، كما جنحت شركة ميكروسوفت " Microsoft " سنة 2021 الى شراء أسهم شركة نيانس " Nuance" بمبلغ 19,7 مليار دولار أمريكي و المستعمل في التعرف على الأصوات من خلل الذكاء الاصطناعي ،مما يعني أن الثورة الرقمية في مجال الصحة أضحت حاضرا و مستقبلا من أهم مصادر الثروة المالية في العالم.

نظرا لخطورة الموضوع وآثاره المدبرة على حياة الناس حين تعرض المستشفيات لهذا النوع من الجرائم، فقد حاولنا استقراء الواقع واستخراج مكونات الجريمة السيبريانية من خلال حصر وتحليل عدد من الأحداث السيبريانية التي مست المؤسسات الصحية في العالم خلال جائحة كوفيد-19.

المنهجية:

لقد تم استحداث استمارة لجمع البيانات تلخص معطيات الجريمة " net-profiler grid of hospitals" مثل المعطيات حول موقع الجريمة وتاريخها، التقنية السيبريانية المستعملة، ودوافع الجريمة وآثارها.

كما تم اعتماد البحث المكتبي الوصفي لدراسة عينة البحث التي حصرت في أحداث ظهور وتطور جائحة كوفيد-19 (2019-2022). كما تم الاستعانة بالتحقيقات الصحفية لدراسة النماذج الاجرامية مثيل دراسة حالة نفسية من خلال آلية التشريح النفسي.

النتائج:

تم تحديد سبعة هجمات سيبريانية على أكبر المجمعات الصحية في القارة الامريكية والأوروبية خلال الفترة الممتدة بين 2019-2022 (الجدول رقم: 1).

جدول رقم 1: الهجمات السيبريانية على المستشفيات

بيانات عامة	التقنية	دوافع الجريمة وآثارها
مستشفى ايسون فرنسا. في أوت 2022	عصابة لوكبيت "Lockpit "	طلب الفدية: 10 ملايين دولار+ نشر لبيانات المرضى بعد شهر من تاريخ الهجمة (11 جيغا)
مستشفى داكس"2 الفرنسي. .8 و9 فبراير 2021 على الثانية صباحا	برنامج كربتولوك برنامج الفدية ريوك	شلل مصلحة العلاج بالأشعة لمدة شهر + كلفة اصلاح العطب /أورو 2 356 000
المجمع الصحي الإيرلندي ماي2021	عصابة كونتي برنامج الفدية ريوك	طلب الفدية: 20 مليون دولار
مجمع الصحي سكريبس " كاليفورنيا .2021.	برنامج الفدية ريوك	سرقة 150 000 ملف + خسارة 113 مليون دولار

المجمع الصحي الأمريكي " . الولايات المتحدة الامريكية. سبتمبر 2020.	العصابة الروسية UNC1878. برنامج الفدية ريوك	67 مليون دولار خسارة مالية في البورصة + 3 أسابيع مدة العطل
المجمع الصحي الإنكليزي."NHS" 2019	" برنامج الفدية ريوك	شلل 50 مؤسسة صحية (20 بالمئة من المجمع الصحي)
.مستشفى الجامعي روان ".بفرنسا 2019	برنامج Cryptomix Clop	شلل لأكثر من 200 تطبيق رقمي + فدية ب 300 ألف أورو

المصدر: نتائج الدراسة للباحث.

في جميع الحالات تمت القرصنة ببرنامج الفدية ريوك" ransomware Ryuk " أو احدى مشتقاته بعد تطويرها. مع الإشارة من خلال التقرير ,2021) (Cert انه منذ سنة 2020 أضحى برنامج الفدية ريوك المتسبب الرئيسي في 78 بالمئة من عمليات القرصنة على المؤسسات الصحية في كل بلدان العالم، وتعتبر الولايات المتحدة الأمريكية وكندا من بين الدول الأكثر مستهدفة ثم تليها إنجلترا وفرنسا.

في كل الحالات، فقد شكل مطلب الفدية المالية وتحويلها الى عملة البتكوين (العملة النقدية الرقمية) القاسم المشترك في عمليات القرصنة.

في معظم الحالات تم تنفيذ التهديد من طرف عصابات القرصنة ولقد عمدت الى نشر البيانات الطبية على منصات البوابة المظلمة.

تمت عمليات القرصنة من طرف عصابات تقبع غالبا في بلدان أوروبا الشرقية.

تحليل النتائج:

مما يتضح أن الجريمة السبريانية من خلال رؤية علم نفس الاجرام تتحدد وفق الأركان الأساسية المكونة لها والتي نوجزها فيما يلي:

1. **الظروف المحيطة بالجريمة**:

1.1. **توقيت الجريمة**: غالبا ما تحدث الجرائم السبريانية التي تستهدف المؤسسات الاستراتيجية والحساسة خلال الليل في فترات محددة حيث تغلب عليها

طابع نقص اليقظة ما بين الفترة الزمنية الثانية والرابعة صباحا. إن الفترة الزمنية هي ميزات لدى مختلف شرائح الاجرام حتى أضحى مجرم الليل " Nightstalker " من بين الصفات الملصقة به والمجرم السيبرياني سمحت له جائحة كوفيد وإجراءات الحجر الصحي بالمكوث مدة أطول في بيته أو مركز عملياته مما سمح له بتأهيل وتوظيف قدراته الذهنية و الفيزيولوجية في مغالبة النوم.

كما تستغل هذه الفترة الزمنية في اختراق خادم الحاسوب " Serveur" ، لتأتي بعدها مرحلة استكشاف الثغرات الأمنية في الشبكة المعلوماتية وغرس البرامج الضارة وتشفير البيانات و الملفات المستهدفة ، مما يستدعي صلابة المجرم السيبرياني الذي أمكن له من الصمود الفيزيولوجي لتحقيق غرضه الاجرامي، حيث دلت بعض حوادث الجرائم السيبرانية على قدرات المجرم السيبرياني بأن يصمد ضد عامل الوقت حتى يتمكن برنامجه من اختراق والتحكم في الهدف المنشود، حيث يمضي لأكثر من 250 ساعة دون أن تستطيع برمجيات الدفاع السيبرياني من كشفه (Shie، 2021).

2.1.**طبيعة المؤسسة المستهدفة**: الجريمة السيبرانية تخص المنشآت الصحية الأكثر رقمنة ومفتوحة على الفضاء الأزرق مع تنوع خدماتها وكثافة تخزين في بنوك حفظ المعلومات الشخصية الخاصة بالمرضى. بالتالي فهي مؤسسات ذات مداخيل نقدية هامة وتشكل مصدر جوهري في عمليات القرصنة مثيل قرصنة المؤسسات الاقتصادية والبنكية. إن طبيعة المعلومات التي يتم قرصنتها من المستودعات الرقمية التابعة للمؤسسات الصحية تحمل من جهة كل المعلومات الخاصة بالمريض " Personally Identifiable Information " وفي نفس الوقت تحمل تفاصيل حياته الصحية (تشخيص طبيعة مرضه، ...) وهذا يشكل أزمة نفسية عميقة الأثر للمعني وبالأخص حينما تكون الأمراض لها وصمة اجتماعية مثل أمراض السرطان أو الأمراض النفسية والعقلية. لهذه المبررات، أضحت مخاوف التهديد بالتشهير على البوابة المظلمة " Dark Web" من أسباب لجوء المؤسسات الاستشفائية وحتى المرضى الى دفع الفدية. حيث تشير الدراسة على تمكن المجرم السيبرياني من بيع الملف الطبي في السوق السوداء بالبوابة

المظلمة بسعر 250 دولار امريكي للوحدة، بالمقارنة تباع البطاقة البنكية بسعر 5 دولار(2020, Minondo) .

يضاف الى الآثار الجماعية و المؤسساتية هو التخوف الشديد من تشويه سمعة المؤسسة المستهدفة و ما يطولها من متابعات قضائية و إدارية بسبب التهاون في حماية بيانات المرضى.

ثم تأتي المؤسسات التي تعني بالتأمين الصحي من بين المنشآت المستهدفة و بالاخص انها تمتلك قدر هائل من الملفات الطبية و محاضر حوادث المرور وغيرها من خصوصيات الملفات التي تعني بها، و بالتالي فهي مرتبطة بمداخيل مالية للتأمين الصحي التي تشكل هدفا مفضلا للهاكرز.

ثم تأتي قرصنة الأجهزة الطبية من بين الأهداف المختارة للقراصنة مثل أجهزة الإنعاش الطبي أو الحقن اللالكترونية التي أضحت من بين الإشكاليات الحساسة للمؤسسات التي تصنع الأجهزة الطبية وبالتالي أضحت الحماية المعلوماتية هاجس قوي للعملاء الصناعيين في حقل الصحة.

كما تمت قرصنة المخابر الدوائية الكبرى و محاولة سرقة حقوق الملكية الفكرية لمنتجاتها ، مثل مخابر صناعة لقاحات ضد كوفيد -19 ، أو الحصول على وصفات طبية تمكن من المتاجرة بالأدوية المهلوسة مثلا.

عموما تشترك مبررات المجرمين في نفس الهدف و هو سرقة الأموال حيث الجشع هو الذي يدفعهم إلى العمل الاجرامي. كما يوضحه تقرير تحقيقات مؤسسة فيريزون لخرق البيانات لسنة 2020، وهي دراسة شملت تحليل 32000 حادث أمني في 81 دولة، و قد تبين انه من بين 10/9 من الهجمات السيبريانية هدفها المال، فيما تعد حوالي 10 بالمئة تخص الجوسسة (2020,D'Ambrosio).

3.1. **المكان الجغرافي**: ان علم الاجتماع الجريمة يسند مدى انتشار الجريمة وتحديد نوعها بحسب تطور المنشآت الفنية و كذا ماهية تطور شبكات الاتصالات مرفقة بمستوى رقمنة القطاع الصحي مثل رقمنة الملف الطبي. فعلى سبيل الاستدلال من خلال تقرير المكتب الفدرالي الامريكي للتحقيقات (Federal Bureau of Investigation ، 2019) أضحت دول شمال أمريكا

و الدول الأوروبية الأكثر عرضة للهجمات السيبريانية و صنفت دول هده المناطق ضمن العشر الأوائل بالرغم من التطور الهائل في الامن السيبرياني.، و بالنالي أمكن القول " هناك تركيز بحثي كبير على بيانات التنميط الجغرافي للمدن المتقدمة في الدول الغربية، ونقص في التحليل والتقديرات لدقة التنميط الجغرافي بالنسبة للبلدان الأقل نموا ذات المظاهر الطبيعية الاجتماعية والاقتصادية والديموغرافية المتباينة (Butkovic ، 2019) .

4.1. **الاستنتاجات**: ان ما اصطلح عليه في حقول البحث ومن زاوية الجريمة الجغرافية أمكن التوسع فيه في فضاء الجريمة السيبريانية التي تعني التزاوج بين المجموعات التابعة والموجهة نحو قطب قيادة مشترك في القرصنة. في الواقع، تعد الجرائم الإلكترونية ظاهرة تتجاهل الحدود الجغرافية التقليدية ولا تستثني أي بلد. يُنظر إليها وفقًا لألشير (El Chear،2003) "على أنها جريمة يكون الكمبيوتر هدفها أو كأداة رئيسية لارتكابها". بمعنى آخر، أن الفروقات الجغرافية ومستوى المعيشة من الجانب الاقتصادي تشكل عناصر مهمة في تركيبة الافراد وتنميط أداورهم، مثلما يمكن مقارنته بين ما يحدث في الجريمة الحضرية وفي الأرياف. ظهرت بعض الملامح النموذجية من التحليلات لدارسات ميدانية والتي أوضحت عوامل مشتركة: ظروف الوصول إلى آلات الكمبيوتر، عدم المساواة الاقتصادية بين الطبقات الاجتماعية، وكذلك سرعة تدفق الإنترنت، وهذا يتوقف على أصل مجرم الإنترنت وهي تدخل في سياق أساليب التنميط الجغرافي " Geographic profiling" (Rossmo، 1997).

ان خلفيات الهدف من الجريمة السيبريانية هو الاشهار الإعلامي وتعزيز لرمز القوة وغزو الويب، فكما يزعم الإرهابيون الإشادة بأسلحتهم العسكرية بنجاح عملياتهم والتغني بجرائمهم النكرة وقتلهم الوحشي من خلال مقاطع الفيديو الدعائية على المنصات للتواصل الاجتماعي، فإن مجرمي الإنترنت ينسخون نفس السلوك من خلال التوقيع الإلكتروني على الصفحات الرسمية المخترقة. بالتالي، فإن الختم المحوسب هو هوية معلنة لمجرم الإنترنت لجذب جمهور كبير وما يجنيه من المتابعة.

هكذا، ظهر مثال مجموعة مجرمي الإنترنت ايرقور "Egregor" في سبتمبر 2020 والتي تجسد أحد الأساليب المتبعة في صياغة الهوية الجماعية لمجرمي الإنترنت. يأتي مصطلح "egregore" من مفهوم مقتصر على فئة معينة، وهو يُستخدم أحيانًا في عالم الإدارة، ويصف "روح المجموعة التي تشكلت من خلال توحيد نوايا وطاقات ورغبات العديد من الأفراد المتحدين لتحقيق هدف محدد جيدًا" (Adam، 2021).

2. سلاح الجريمة من خلال تقنية القرصنة ووسائلها:

1.2.**سلاح الجريمة**: في أغلب الحالات تم استعمال البرامج ذات خلفية للابتزازات المالية من خلال طلب فدية من إدارة المؤسسات الصحية، وهذه البرامج الفدية " ransomware " أضحت الهاجس الأكبر للمختصين في الأمن المعلوماتي لانتشاره السريع والمكثف خلال هجمات الهاكرز. على سبيل الاستدلال ذكر المعهد الدولي " Cyberpeace Institute " الى إحصاء 445 هجمة سيبريانية على المؤسسات الصحية خلال الفترة الممتدة بين 2 جوان 2020 و20 جوان 2022 ((2022,Cyberspace. في نفس السياق أشارت شركة سوفوس " Sophos "في دراسة إحصائية للجريمة السيبريانية ضد المؤسسات الصحية الى كشف أن 66 % من المنظمات الصحية المستجوبة تعرضت الى هجمات سيبريانية خلال سنة 2021 مقارنة ب 33 % سنة 2020 وأن حوالي ثلث المؤسسات الصحية المستهدفة دفعت فدية مالية الى الهاكرز حتى تتمكن من استرجاع بياناتها (2022,Sophos).

2.2.. **أساليب ارتكاب الجريمة**: من بين التقنيات الأكثر شيوعا هي اللجوء في المرحلة الأولى من القرصنة الى التصيد الاحتيالي، حيث يتفوق مجرمي الإنترنت اليوم في سرقة بيانات تحديد الهوية " identification data "، سواء من خلال تقنيات التصيد الاحتيالي " phishing " أو ببسط القوة الغاشمة (بفضل ممارسة إعادة استخدام كلمة المرور على نطاق واسع).

لقد تعلم مجرمي الإنترنت أن يكونوا أكثر صبرًا بعد التسلل إلى النظام المعلوماتي المستهدف وأن يأخذوا الوقت الكافي لتحليل ضحاياهم وتوصيفهم.

فعلى سبيل الاستدلال ووفقًا لأحدث تقرير عن تكلفة خرق البيانات لشركة ايبيام "IBM »، يستغرق حادث الاختراق من المؤسسات الضحية ما متوسطه 280 يومًا لتحديد واحتواء خرق البيانات. بمعنى آخر، لأكثر من 9 أشهر، يمكن للمجرم السيبرياني موجود على الشبكة التخطيط لأفعاله قبل توجيه ضربة قاضية له.

تتراوح نتيجة هجوم التصيد الاحتيالي الناجح من بيانات الاعتماد المخترقة إلى تشغيل حصان طروادة" Trojans" للوصول عن بُعد للكمبيوتر. عندما يتعلق الأمر بتصيد بيانات الاعتماد، فقد لجأ المجرمون الإلكترونيون مؤخرًا إلى استخدام نطاقات فرعية قابلة للتخصيص للخدمات السحابية المعروفة لاستضافة نماذج مصادقة ذات مظهر شرعي.

كما تجدر الإشارة انه خلال جائحة كوفيد -19 تم استغلال رموزها في مختلف رسائل الاصطياد بعنوان تشخيص الداء أو اقتراح علاج ناجع وفي بعض الأحيان المطالبة بالمساعدة أو التبرع المالي في فائدة ضحايا الجائحة أو المساهمة في البحث العلمي لإيجاد اللقاح المضاد لها. من جهة ثانية، فقد انفردت بعض المجموعات من القراصنة في تطوير برامج فدية الخاصة بها والتي تحمل اسم فيروس كورونا-19.

في حالة هجمات للبرامج الضارة على شاكلة التصيد الاحتيالي، توقف المتسللون الأكثر نجاحًا إلى حد كبير من إرفاق برامج ضارة قابلة للتنفيذ برسائل البريد الإلكتروني الخاصة بهم، لذلك يفضل مجرمي الإنترنت استخدام ملفات القطارة" dropper»، والتي تأتي عادةً في شكل مستندات مايكروسوفت اوفيس" Office Microsoft " تحتوي على وحدات ماكرو"Macro" أو ملفات جافا سكريبت" Java Script".

كما تستعمل تقنية التحايل المطبعي " typosquatting" التي تعتمد على الهندسة الاجتماعية لخداع مستعمل النت، وبالتالي جره نحو روابط النت السيبريانية واصطياد عناوين البريد الالكتروني وحتى كلمات السر للزبائن.

كما اتخذت عصابات الاجرام السيبرياني تقنية الرسائل المبعثرة "scattergun " التي استعملتها عصابة ت.أ.505. " TA505" في الهجوم على

المستشفيات، حيث بعثت أكثر من 000 200 رسالة خبيثة الى مخابر صيدلانية و50 مليون ملف خبيث في يوم واحد(2020,Guezo) .

تصبح الأمور أسهل إذا تمكن المتسللون من سرقة بيانات اعتماد أو تحديد هوية صالحة ولم تنشر الشركة مصادقة متعددة المستويات. من ثم يتم فتح البوابة الرقمية للشبكة على مصراعيها، مما يمكنهم بعد ذلك من الاستفادة من خدمات الضحايا مثل محركات البرمجة النصية المضمنة في الويندوز" Windows".

في المرحلة الحاسمة يتم تشفير البيانات مع الامضاء الخاص بالمجرم عن طريق رسالة يوضح فيها كنيته السبريانية، هدفه ومطالبه.

من بين البرامج الضارة لطلب الفدية " ransomwer" التي تم الكشف عنها في عمليات قرصنة بيانات المؤسسات الصحية في العالم يوجد أكثر من 18 نوع، نذكر من بينها: بلاك كات " BlackCat " ، كانتوم " Quantum "،هايف " Hive "، افوسلوكار" AvosLocker ".

كما تم استعمال البرامج لطلب الفدية " ransomwer" باستغلال جائحة كوفيد 19، فبرنامج التصيد الاحتيالي أزور ايل "AzorUlt " كان يقترح خريطة انتشار جائحة كورونا-19 بواسطة الرسائل الإلكترونية، أو ايموتات " Emotet" الذي يتموه باسم المساعدة الاجتماعية للمعاقين.

بعد التهديد بنشر البيانات في حالة رفض الضحية دفع الفدية، يتم نشر البيانات في البوابة المظلمة " dark Web " أو على روابط المواقع " leaks site " أو حتى الفضاء الأزرق المتاح للجميع. غالبا ما تتم عمليات الحسم بعد القرصنة من طرف مجموعة المجرمين التي منحت لأنفسها أسماء، مثل: مجموعة ماز " Maze "، مجموعة كلوب " Clop " ، مجموعة دوبل بيمر " Dopplepaymer "، مجموعة نيفيليم " Nefilim" ، مجموعة نمتي " Nemty " ، مجموعة رنيا لوكر " Ragnalocker " ، مجموعة ريفيل " Revil " ، مجموعة سخمات " Sekhmet" و غيرها.

3.2. **الاستنتاجات**: مما تم ذكره، أمكن الجزم بأن المجرم السيبرياني أضحى متكيف مع العالم الذي يعيش فيه وليس نمطيا مثل ذلك الانسان المنعزل

عن الأحداث، وطالما أن الإبحار في الفضاء الأزرق لا يحتاج الى شهادات رسمية من مؤسسات التكوين الأكاديمي، وبالتالي أضحت فئات المهاجمين المختصين تطور باستمرار كيفيات ابتكار أساليب نوعية من خلال محاولات التصيد "phishing" عن طريق اللعب على المحفزات العاطفية، مثيله في ذلك في حملات الابتزاز الجنسي " sextorsion " حيث يستغل مجرمي الإنترنت في إحراج ضحاياهم وتخويفهم من ابتزاز أموالهم بسبب الخشية وعدم اليقين من وضعهم الصحي الحالي، فقد أوجد المجرمون السيبرانيون عواطف رئيسية و مفتاحية لاستغلالها.

من هذا المنطلق، فان دراسة ممارسات الهندسة الاجتماعية " social engineering" بمسميات علم النفس السيبرياني التحايل أو الغش النفسي " psychological fraud " حيث "كشفت الأبحاث أن المحتالين يجدون المتعة، التي غالبًا ما تكون مستمدة من الشعور بالتفوق في الهجمة الصعبة على شخص آخر، والتي قد تكون بمثابة عامل محفز لارتكاب متكرر لهذه الأنشطة الإجرامية « ((2022,Pimentel.

يُطلق على القرصنة النفسية أيضًا عملية الاستنباط " elicit"(من الاستنباط الإنجليزي: الفرز، والخروج من، والإثارة، وما إلى ذلك)، أو فن الاستخراج الاحتيالي للمعلومات دون علم المحاور. غالبًا ما يستخدم هذا المصطلح في لغة الكمبيوتر للإشارة إلى عملية النهج العلائقي الاحتيالي ويحدد بشكل عام الأساليب التي تنفذها بعض القراصنة (المتسلل أو القبعة السوداء) Crackers "" ، الذين يستخدمون "الاستنباط" للحصول من شخص تم التحايل العلائقي عليه بهدف الوصول المباشر إلى جهاز كمبيوتر أو من اجل إرضاء فضولهم.

3. نمط شخصية المجرم السيبرياني:

1.3. **الهيكلة والخصوصيات الجماعية للجريمة السيبريانية**: توجد آليات هيكلية يمكنها من إلقاء الضوء على الظاهرة الاجرامية، حيث تعمل معظم مجموعات برامج الفدية اليوم وفقًا لنموذج تقسيم المهام والأدوار: فمن ناحية، يقوم ما يسمى بالمشغلين بتطوير وصيانة البرامج الضارة والبنية التحتية المحيطة بها، وتأجير هذه الخدمات إلى قراصنة آخرين، يطلق عليهم الشركات التابعة.

هذه الفئة الثانية المتخصصة في اختراق الكمبيوتر، ليسوا دائمًا أعضاء كاملين في "السفينة الأم"، ولكن يمكن اعتبارهم مقاولين يعملون مع مجموعات مختلفة. ومع ذلك، فإن هذه الجهات الفاعلة المختلفة ليست بالضرورة على نفس الخط وتظهر للعلن وعلى صفحات التواصل ردود أفعال متباينة لأعضائها.

بمعنى آخر، فإن خريطة الاجرام السيبرياني تنسخ مثيل تشكيلة مختلف العصابات الاجرامية مهما تنوعت طبيعة جرائمها. فالرؤوس الكبيرة تشكل مركز القوة حيث تستمد نفوذها من عدة عوامل: انها صاحبة ابتكار البرامج السيبريانية الضارة أو تتحكم في المنصات التي تمكنها من توسيع شبكات المنضمين اليها، أو تعتمد على مصادر قوة من خلال عمليات تبييض الأموال ذات المصدر الاجرامي (التجارة في المخدرات، في السلاح، في المسروقات الباهظة الثمن ،....). ثم يأتي المقام الثاني للعملاء، وكل حسب درجات كفاءته فتسند له مهام بالأخص في شن الهجمات المتكررة وبمجموعات كثيرة العدد ومن مختلف المناطق الجغرافية، و كما وصف من زاوية علم الاجتماع الجريمة " أن المجتمع الرقمي صنع حجم التحايل" (2022,DiNicola) .

من خصوصيات الخريطة الاجرمية أن الهوية الحقيقية لأصحابها غير معلومة حتى فيما بين أعضائها و يصعب كشف هويتهم بسبب استعمال الأسماء المستعارة، كما تتم عمليات التواصل فيما بينهم من خلال البوابة المظلمة أو منصات المحادثة غير مفهرسة في محركات البحث العادية " darknets ".

إن عمليات قرصنة البيانات تتبعها سلوكيات التهديد والتشهير ضد الضحايا أو تباع " المسروقات " في السوق السوداء و غير رسمي في البوابة المظلمة " Darknet markets " التي تعتمد فيها العملة النقدية الرقمية "بتكوين" " bitcoins"كطريقة كسب غير قانونية ودون أن تترك لها أي آثر للمتابعة القضائية. هذا المسار الاجرامي يعكس التطابق الكلي بين الجريمة السيبريانية مع مختلف الجرائم " التقليدية" التي تسري على وجه الأرض (السرقة، التجارة بالأسلحة و المخدرات،...).

2.3. **عوامل السن و النمو النفسي كمحددات لدى المجرم السيبرياني**: من مجموع زوايا التنظير لعلم النفس الاجرام، نذكر نظرية بفيرن " Beveren"

(2001,Beveren) التي توضح أن الميل الذي يقود المخترق إلى اللجوء نحو السلوك الإجرامي أثناء تطوير مهاراته في هذا المجال. وبناءً عليه، تم تقسيم دوافع الاختراق إلى أربعة محاور: الإكراه على الاختراق، الفضول، السيطرة والشغف للسلطة، التعرف على الأقران والانتماء إلى المجموعة.

يفترض النموذج أن غالبية المتسللين يباشرون العمل الاجرامي كمبتدئين مثل قرصنة كلمة السر للبريد الالكتروني، قبل اكتساب المزيد من المهارات والمعرفة والخبرة ليصبحوا محترفين. هذا المسار الاحترافي يوضح أنه مع تطوير المتسللين لمهاراتهم، قد تتطور أيضًا النوايا والدوافع وراء أنشطتهم المتعددة، وكما هو معلوم أن "الدافع يشكل باختصار الخلفية النفسية للنية" في الفعل الاجرامي2014) (Pradel,. كما أشارت الدراسات حول نمط المجرم السيبرياني في بداية القرن الواحد والعشرون على أنهم معتمون وغير مهتمين بأنفسهم ومعادون للمجتمع، ولديهم مهارات اجتماعية ضعيفة، أو نشأوا في أوساط أسر مختلة(2006, Rogers) ، ولديهم سلوك ادمان على النت منذ الصغر (Dupont, 2013). لكن التطور التكنولوجي واختصار طرق الوصول الى مكامن التكسب غير شرعي قلب معايير التنميط التقليدي.

لكن وجب التنويه أن العوامل النفسية والاجتماعية هي أساس الفهم الصحيح لسلوكيات الفرد من خلال بيئته الأصلية، وعليه فان الطفل يولد على الفطرة السليمة وبالتالي خصوصيات بيئته الوالدية والأسرية هي مفاتيح لفهم تطوره النفسي، ثم تتصدر الفروقات الفردية من الفطانة والذكاء الخارق وغيرها من ملامح ما يسمى بالأطفال المواهب في شتى المعارف هي من بين المؤديات لدى البعض في تبني بشغف وكبير في طرق التحكم في تقنيات الاعلام الالي و الابحار في المواقع حتى تصبح اللعبة المفضلة بين أيديهم، مما يفسر تصنيف المجرمين في هذه الفئة العمرية ب"سكربتات صبيانية أو طفولية" " script kiddies ". انها تستعمل برامج تفتقر الى مهارات التشفير عموما مما يتيح لكشفهم بسهولة من طرف الجهات الأمنية، وهنا فالنصوص الطفيلية تعتدي على المواقع بغية الاثارة واعلاء سمعتهم بين أقرناهم.

كما يتم التنظير لعلم النفس السيبرياني من خلال علوم سلوك الانسان التي تشير إلى عمليات التقليد الذهني والتمثلات الاجتماعية التي تشحن بها دوافع المجرم السيبرياني والتي تجعل من مصادر إلهامها وتشكيل القدوة الاجتماعية برمزيات العدالة الاجتماعية أو الوطنية وغيرها من النماذج التي تتشبع بها دائرة الطفل أو المراهق.

أما من زاوية الأنثروبولوجيا الجنائية، فقد تتشكل لنا مصادر مكملة لفهم سلوك المجرم السيبرياني في الأوطان العربية مثلا، الذي قد يتغدى من انعدام وسائل التكفل الطبي في المستشفيات العمومية وارتفاع تكلفة العلاج في المصحات الخاصة، فتصبح عناوين له ومحفزات لتشكيل ورقة مهمة وجب الوصول لأهدفا بدافع تحقيق العدالة الاجتماعية.

كما أضحى لهذه الفئة العمرية أن تسلك طريق الخير بتعمد إنتهاج التعدي على شبكات الأنظمة والاتصالات لإبراز عناصر التفوق الشخصي مثل فئة المجربين لأمان الشبكة المعلوماتية " pentesters ".

فإذا كانت عصب الإرهاب تجند ضمن صفوفها كل فئات المجتمع، فنفس الأمر ينطبق على هيكل الجريمة السيبريانية حيث تجتمع العصابة على هدف قرصنة جهاز كمبيوتر فرد أو المشاركة في هجمات واسعة النطاق ضد مواقع حكومية أو مؤسسات رسمية، وقد دلت الدراسات على مشاركة الأطفال مثلا في دولة كوت ديفوار حينما اعتقلت الجهات الأمنية مجموعة من القراصنة تتراوح أعمارهم ما بين 12 و 25 سنة (Bogui, 2010) .

في نفس سياق دراسة فضاءات الجريمة السيبريانية التي لا تخرج عن منطق سلوك الإنحراف، حيث يفضل المجرمون ارتكاب الجرائم في فضاءات وعيهم لأن هذه الأماكن مألوفة لديهم (2022,Dongping). فقد كانت ظاهرة انتشار مقاهي الانترنت تشكل احدى مصادر تكوين عصابات النت و بالأخص في البلدان الفقيرة .

مقارنة مع خريطة الجرائم "التقليدية " ، فان المجرم السيبرياني عوض أن يعتاد المناطق الحضرية الأكثر نشاطا مثلما يحصل لدى السارق " تكون المخاطر عالية بشكل خاص إذا كانت المناطق تحتوي على عقد نشاط يتردد عليها مجرمون

محتملون متحمسون " (Menting, 2020) ، فانه يعتاد الانضمام الى منصات المحادثة أو منتديات الدردشة و غير المفهرسة لدى الشخص الاعتيادي حتى يصقل معارفه و يوسع شبكة التواصل و التوغل في البوابة المظلمة..

3.3.عوامل المهارات الذهنية و النفسية محددات في ترقية مسار المجرم السيبرياني: على أساس هذه الفروقات عمد الباحثون على تصنيف المجرم السيبرياني الى تسع فئات رئيسية: المبتدىء "Novice " ، الأشرار السيبريانية " Cyber-punks " ، السيبراني الداخلي أو الانتقامي " Internals " ، اللصوص الصغار"Petty Thieves " ،كتاب الفيروسات" Virus Writers " ،قرصان الحرس القديم " Old Guard hackers " ، المجرم المحترف " Professional Criminal" ،محارب المعلومات " Information Warrior " و الناشط السياسي " Political Activist "(Marcus، 2006).

فالمبتدئون ينخرطون في عالم الهاكرز بدافع غريزة الفضول وتحفزهم التحديات الفكرية وغالبا نجد ضمنهم المولعون بالإعلام الألي أو الألعاب الإلكترونية، و هنا تستوقفنا محطة النمو النفسي-الحركي فيما يخص الأطفال الموهوبين الذين يوصفون " بالاهتمام والتركيز الفائق والتمتع بالعمل الفكري....لكن قد يفشلون في مسارهم الدراسي لعدم تكيف مستوى ذكائهم بمحيطهم المدرسي "(1990,Beverina). مما لا شك فيه أن النوابغ في عالم النت و الرقمنة انضموا الى عالم القرصنة ، ربما بمسميات متنوعة و أهداف مشبوهة ، لكن مع الوقت فقد أضحى الاجرام السيبرياني يشكل متنفس لهم و وسيلة هروب من الروتين اليومي و التقليد الحياتي ، فكأن لهجماتهم السيبريانية واجهة تمثل سلوك انتقامي ضد مؤسسات المجتمع أو رمز قوة أو شهادة رد اعتبار أو إعادة الاعتبار المجتمعي.

لكن ما يلاحظ من هذه الأمثلة من التقسيمات انها مؤسسة على طبيعة الجرم، سن المجرم، الأقدمية في مسار الجريمة ومبررات الجريمة. انها عناصر متداخلة وقد تكون غير متناسقة طالما أن عامل الوقت والمحفز الشخصي للمجرم هو الذي يمكنه من الحصول على صفة المبتدئ أو المحترف.

إن تتبع الجرائم المتعددة وتمحيص نمط المجرم يدلنا أن البيئة الأسرية والمحيط القريب خلال نشأة المجرم السيبرياني تبدو من العوامل التي تنحرف بالمراهق نحو الجريمة السيبريانية.

ان الاستئناس بالبحث التاريخي حول الجريمة السيبريانية يشير أن هجمات برامج الفدية استهدفت الأفراد، الشركات والحكومات لعقود. لقد تم إطلاق أول هجوم موثق لبرامج الفدية، والمعروف باسم حصان طروادة -ايدز " AIDS Trojan " أو كمبيوتر سايبورغ " Cyborg PC"، في عام 1989 من قبل جوزيف بوب، عالم الأحياء التطوري المتدرب في جامعة هارفارد. لقد قام بوب بتخزين الفيروس على أقراص مرنة كانت تحتوي على برنامج تعليمي عن الإيدز، ثم أرسلها بالبريد إلى ضحاياه. بمجرد التنشيط، قام برنامج الفدية " AIDS Trojan ransomware " بتشفير الملفات على كمبيوتر الضحية وطالب بفدية قدرها 189 دولارًا لإلغاء تأمينه(2021,Murphy Kelly) . و في نفس السياق نذكر الطبيب المختص في أمراض القلب، الطبيب مويس لويس زقالا قونزاليس" Moises Luis Zagala Gonzalez" الذي تم القبض عليه سنة 2019 بتهمة تطوير برنامج فدية تانوس " Thanos ransomware" و التشهير بفاعليته و نجاعته في فضاء البوابة المظلمة حيث استهدف المؤسسات الصحية في عدة بلدان من العالم (2022,Thierry).

في هذا النوع من الاجرام السيبراني تم الاستدلال بمهنة وطبيعة التكوين الأكاديمي لمن امتهن الطب، لكن انشغل بالموازاة بفنون الاعلام الالي وانغمس في سلوك الاجرام كنوع من التلذذ في السيطرة والتحكم. هذه الأمثلة من الجرائم السيبريانية توضح ماهية فئة من كوادر الصحة المجملة في "الأطباء المجرمين "Killers doctors "الذين انحرفوا بمعارفهم وعبثوا بضمائرهم واخلاقيات ممارسة مهنتهم، شأنهم مثيل قضية جراح الأعصاب الأمريكي " كريستوفر دونتش " Christopher Duntsch " المتهم بقتل مرضاه عمدا، فقد أوضحت دراسة محتوى للسلسلة التلفزيونية "الطبيب القاتل" " Dr.Death " ماهية نمط شخصيته: نرجسي، سلطوي ونفيه للخطأ أي معصوم من الخطأ (2022,Hachelafi).

من جهة ثانية، فأمثلة الاستدلال توضح ان المهارات الفنية في القرصنة لا تعكس المستوى العلمي التقليدي للمجرم السيبرياني. مثال ذلك المقبوض عليه سيبستيان غاول" Sébastien Raoult " الفرنسي الجنسية و صاحب 21 سنة و المتهم بالانتماء الى العصابة السيبريانية شيني هانترز " ShinyHunters "، حيث أوضحت التحقيقات الصحفية أنه منذ سن التاسعة فقد لزم المتهم جهاز الكمبيوتر في تحضير دروسه و لم يواصل دراسته الجامعية في المعهد الخاص بالإعلام الألي و انقطع عنها مبكرا ليتفرغ لهويته المفضلة (De Labarre، 2022).

4. واقع و تحديات السيبريانية في العالم العربي:

مما لا شك فيه أن خصوصيات الجريمة السيبريانية التي لا تعترف بالحدود المرسمة بين البلدان تمهد الى إفلات رؤساء العصابات من الحجر الأمني المفروض عليهم في البلدان الأكثر تقدما في مجالات الحماية السيبريانية حيث تفرد حكوماتها مبالغ مالية من أجل تطوير أساليب مكافحتها والترصد لتحركاتها ليتم التخفيف من آثار هجماتها. على سبيل الاستدلال هو تفرغ قيادة الأركان في البلدان الغربية بفتح مديريات عسكرية متخصصة في الأمن السيبرياني مع تعدد المهام في الصد والترصد وهي خلايا تابعة لمختلف فروع الأسلحة البرية، البحرية والجوية.

إن خريطة الجريمة السيبريانية أضحت تتغير بحسب الظروف الأمنية وتطور أساليب مكافحة الجريمة وعليه تشير تقارير منظمات الأمن السيبرياني أن بعض بلدان القارة الإفريقية مثلا أضحت ملجأ لعصابات الجرائم الإلكترونية مع سهولة التنسيق مع الأفراد أو المجموعات الاجرامية المحلية، بالإضافة إلى صعوبة ملاحقتها والكشف عن هويتها من طرف أجهزة الأمن المتخصصة المحلية. حيث منذ عشرات السنوات، في عام 2010، صنف قسم الجرائم السيبريانية التابع لمكتب التحقيقات الفيدرالي الأمريكي (FBI) ثلاثة بلدان إفريقية من بين المصادر العشرة الأولى لعمليات الاحتيال الإلكتروني: نيجيريا (المركز الثالث)، غانا (المرتبة السابعة) والكاميرون (المرتبة التاسعة)(Ben Hadid, 2022) . كما كشفت تقارير الأمن الدولية إلى ضلوع عدة أفراد تنتمي إلى الوطن العربي

تمكنت من الانضمام الى الشبكات الدولية والمشاركة في هجمات القرصنة أو في شكل عمليات فردية مست هيئات حكومية ورسمية في البلدان العربية وتجاوز صدها حدود بلدها الأصلي، مثل هجوم عصابة الأشباح المغربية " Moroccan Ghosts" على موقع الشرطة لجنوب افريقيا (2012,Amar)و حتى على المواقع الحكومية الجزائرية بخلفية أنها مصنفة ضمن الهاكرز النشطاء " Hacktivist" (Khefifi, 2013).

انه من دواعي التطور التكنولوجي اللجوء الى تحصين المؤسسات الصحية بالأخص أن الثورة الرقمية ستمس ملزمة باستخدام تطبيقات وأجهزة الفحص العيادي والمتابعة العلاجية في الوطن العربي مما يستدعي التكفل الجاد بهذه الزاوية التي أغفل الخبراء التعامل معها من جانب وقائي واحترازي.

إن الحرب الضروس السيبريانية أضحت من الأهداف السامية والحيوية لدى قيادات الجيوش العالمية ، وبالتالي إمكانية استعادة الموهوبين الشباب في الاعلام الالي والتكفل بهم منذ نعومة أظافرهم لتجنيدهم بشكل متعدد يسمح بتقوية السند اللوجستيكي ويسحق بصفة مبكرة لمحاولات القرصنة عن بعد ، مثلما تشير اليه تسميات المحاربون السيبرانيون " cyber- warriors " ,2012) .Ventre)

كما تشير الاحصائيات من خلال التقرير الذي يسلط الضوء على الاختراق الرقمي لدول العالم، بما في ذلك منطقة الشرق الأوسط، حيث بلغت نسبة مستخدمي الإنترنت حوالي 70٪ عند 182.1 مليون مستخدم، في المقابل، بلغ عدد مستخدمي مواقع التواصل الاجتماعي في المنطقة حوالي 125.4 مليون شخص، أي 48٪ من السكّان. ومن المنطقة العربية ، جاءت دول الإمارات العربية المتحدة، قطر، الكويت والبحرين في مقدمة دول العالم والشرق الأوسط على قائمة الدول الأعلى اختراقاً ووصولاً للإنترنت (2021,Arabia)، مما يستدعي وضع إستراتجية أمنية جادة لتطوير آليات الأمن السيبرياني وعلى مختلف المستويات الاجتماعية فهي مسؤولية جماعية.

□

الخاتمة:

ان تنميط المجرم السيبرياني يستدعي دراسات أكاديمية تدمج بالأخص العوامل النفسية والاجتماعية في الوطن العربي حتى تتمكن من تقليل عمليات التجنيد وتفادي العواقب الوخيمة ذات الأبعاد المتعددة حين تعرض المؤسسات الحكومية أو الخدمات الى هجمات سيبريانية.

لقد برعت جهود الأمن السيبرياني في مكافحة الجريمة على صعيد دولي متناسق، وتكاثفت الاجتهادات في مراكز البحوث والدراسات الجامعية من أجل حصر آثارها والوقاية منها، مثل جهود علم التشريح الجنائي في تشخيص البصمة الدماغية «Forensic brainwave analysis" لدى المجرم (Bettayeb, 2018).

المراجع:

Adam, L. (2021, janvier 8). *Ransomware : Egregor, la relève cybercriminelle.* Récupéré sur ZDnet: https://www.zdnet.fr/actualites/ransomware-egregor-la-releve-cybercriminelle-39915873.htm

Amar, A. (2012, November 9). *Ces hackers marocains qui font trembler la Toile.* Récupéré sur SlateAfrique: http://www.slateafrique.com/97729/qui-se-cache-derriere-moroccan-ghosts-hacker-cyber-activiste

Arabia, C. (2021, March 14). *كيف كان أداء الدول العربية من حيث الاختراق الرقمي في عام2020* ؟

Ben Hadid, N. (2022, juillet 05). *L'Afrique et la cybercriminalité: Triste palmarès!* Récupéré sur La Majalla: https://fr.majalla.com/node/237216/reportagesl%E2%80%99afrique-et-la-cybercriminalit%C3%A9-triste-palmar%C3%A8s

Benbouzid, B., & Ventre , D. (2016). Pour une sociologie du crime en ligne. *La Découverte, 3*(197-198), pp. 9-30. doi:10.3917/res.197.0009

Bettayeb, K. (2018, November 19). L'analyse des ondes cérébrales des criminels. *Science & Vie*(263).

Beveren, J. (2001). A conceptual model of hacker development and motivation. *Journal of E-Business, 1*(2).

Beverina, M. (1990). Les enfants surdoués une chance ou une fragilité? *Journal de Pédiatrie et de Puériculture, 3*(2), pp. 87-92. doi:10.1016/S0987-7983(05)80432-3

Bogui, J.-J. (2010). La cybercriminalité, menace pour le développement. *Afrique contemporaine, 2*(234), pp. 155-170. doi:10.3917/afco.234.0155

Butkovic, A., Mrdovic, S., Uludag, S., & Tanovic, A. (2019). Geographic profiling for serial cybercrime investigation. *Digital Investigation, 28*, pp. 176-182. doi:10.1016/j.diin.2018.12.001

Cert. (2021, September 01). *Le rançongiciel Ryuk*. Récupéré sur https://www.cert.ssi.gouv.fr: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-011.pdf

Cohen, D., Hung, A., Weinberg , E., & Zh, D. (2020, December 01). *Healthtech in the fast lane: What is fueling investor excitement?* Récupéré sur mckinsey.com: https://www.mckinsey.com/industries/life-sciences/our-insights/healthtech-in-the-fast-lane-what-is-fueling-investor-excitement

Cyberspace, I. (2022). *Cyber Incident Tracer #HEALTH.* Récupéré sur Cyberspace Institute: https://cit.cyberpeaceinstitute.org/explore

D'Ambrosio, M., & Force Hill, J. (2020, Mai). *Verizon Data Breach Investigations Report 2020.* Récupéré sur https://www.verizon.com: https://www.verizon.com/business/resources/reports/2020-data-breach-investigations-report.pdf

De Labarre, F. (2022, Aout 21). *Sébastien Raoult, un Français dans les griffes du FBI.* Récupéré sur https://www.parismatch.com: https://www.parismatch.com/Actu/Societe/Sebastien-Raoult-un-Francais-dans-les-griffes-du-FBI-1821851

Di Nicola, A. (2022, May 30). Towards digital organized crime and digital sociology of organized crime. *Trends Organ Crim*. doi:10.1007/s12117-022-09457-y

Dongping, L., & Lin , L. (2022). Do juvenile, young adult, and adult offenders target different places in the Chinese context? *Cities, 130*. doi:10.1016/j.cities.2022.103943

Dupont, B. (2013). Skills and trust: a tour inside the hard drives of computer hackers. Dans C. Morselli, *Illicit networks* (pp. 195-217). London, United Kingdom: Routledge.

Federal Bureau of Investigation, F. (2019). *internet crime report*. Récupéré sur https://pdf.ic3.gov/2019_IC3Report.pdf

Guezo, L. (2020, mai 24). *Pourquoi le secteur de la santé reste une cible privilégiée pour les cybercriminels ?* Récupéré sur https://www.apssis.com/: https://www.apssis.com/actualite-ssi/517/pourquoi-le-secteur-de-la-sante-reste-une-cible-privilegiee-pour-les-cybercriminels.htm

Hachelafi, H. (2022, June 10). Content study of a medical television series. *Revue Afaque Cinemaia, 9*(1), pp. 42-59. Récupéré sur https://www.asjp.cerist.dz/en/downArticle/158/9/1/192121

Khefifi , W. (2013). Moroccan Ghosts . *Réseau Télécom*(63).

Lederer, E. (2020). Top UN official warns malicious emails on rise in pandemic. Récupéré sur https://apnews.com/article/c7e7fc7e582351f8f55293d0bf21d7fb

Marcus K. Rogers. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation, 3*(2), pp. 97-102. doi:10.1016/j.diin.2006.03.001

Menting, B., Lammers, M., Ruiter, S., & Bernasco, W. (2020). The influence of activity space and visiting frequency on crime location choice: Findings from an online self-report survey. *The British Journal of Criminology, 60*(2), pp. 303-322.

Minondo, T. (2020, august 20). *Intelligence artificielle : une société spécialisée laisse fuiter 2,5 millions de dossiers médicaux*. Récupéré sur Siécle digital: https://siecledigital.fr/2020/08/20/intelligence-artificielle-une-societe-specialisee-laisse-fuiter-25-millions-de-dossiers-medicaux/

Murphy Kelly, S. (2021, Mai 16). *The bizarre story of the inventor of ransomware*. Récupéré sur https://edition.cnn.com/:

https://edition.cnn.com/2021/05/16/tech/ransomware-joseph-popp/index.html

Pimentel, A., & Steinmetz, K. (2022). Enacting social engineering: the emotional experience of information security deception. *Crime Law Soc Change, 77*, pp. 341-361. doi:10.1007/s10611-021-09993-8

Pontier , N., & al. (2022, October). Cyberattack at Dax hospital: Presentation of the facts, consequences and feedback. *Cancer / radiothérapie, 26*(6-7), pp. 938-940.

Pradel, J. (2014). *Droit pénal général*. France: Cujus.

Rogers, M. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation, 3*(2), pp. 97-102. doi:10.1016/j.diin.2006.03.001

Rossmo, D. (1997). Geographic profiling. Dans J. L. Bekerian, *Offender profiling: Theory, research and practice* (pp. 159-175). United States: John Wiley & Sons Inc.

Shie, J., Gangwer, M., Iddon, G., & Mackenz, P. (2021, Mai 18). *The Active Adversary Playbook 2021*. Récupéré sur news.sophos: https://news.sophos.com/en-us/2021/05/18/the-active-adversary-playbook-2021/

Sophos. (2022). *The state of ransomware in healthcare*. Récupéré sur New Sophos: https://news.sophos.com/en-us/2022/06/01/the-state-of-ransomware-in-healthcare-2022/

Thierry, . (2022, Mai 17). *Ransomware : Pourquoi la justice américaine vient d'inculper un cardiologue franco-vénézuélien*. Récupéré sur https://www.usine-digitale.fr: https://www.usine-digitale.fr/article/ransomware-pourquoi-la-justice-americaine-vient-d-inculper-un-cardiologue-franco-venezuelien.N2005592

Ventre , D. (2012). Le cyber-guerrier : nouvelle figure combattante au service de la cyber-défense. *Sécurité et stratégie, 4*(11), pp. 96-48. doi:10.3917/sestr.011.0039

Wisecase. (2019, October 21). *Data Leaks in the Medical Industry: A Worldwide Epidemic*. Récupéré sur https://www.wizcase.com: https://www.wizcase.com/blog/medical-breaches-research/